Customer No.36,547

PATENT

☒ *OFFICIAL*
☐ *UNOFFICIAL*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): David S. Colvin

Serial No: 10/605,061 Group Art Unit: 2131

Filed: 05 Sep 2003 Examiner: Revak, Christopher A

Title: HARDWARE BASED METHOD FOR DIGITAL RIGHTS MANAGEMENT INCLUDING SELF ACTIVATING/SELF AUTHENTICATION SOFTWARE

Attorney Docket No.: COL404PUS Confirmation No.: 2060

APPEAL BRIEF UNDER 37 C.F.R. §41.37

Sir:

Applicant requests a 4-month extension of time for a small-entity and has paid the appropriate fee in addition to the fee for filing this brief in support of the Notice of Appeal filed June 5, 2007.

Applicant is appealing the final rejection of all claims 1-99 under 35 USC §103(a) for consideration by the Board of Patent Appeals and Interferences and requests the final rejection of claims 1-99 as being unpatentable over Ananda (US 5,495,411) in view of Garceau et al ("General Controls in a Local Area Network") be reversed and this case be remanded with instructions for passing to issuance.

(i) REAL PARTY IN INTEREST

The real parties in interest for this application are the applicant David S. Colvin and the assignee, z4 Technologies, Inc..

(ii) RELATED APPEALS AND INTERFERENCES

There are no prior or pending appeals, interferences or judicial proceedings known to applicant or the assignee that are related to, may directly affect, may be directly affected by, or may have a bearing on the Board's decision in the pending appeal.

(iii) STATUS OF CLAIMS

Claims 1-99 are currently pending in this application and have been rejected under 35 USC §103(a) as being unpatentable over Ananda, U.S. Patent 5,495,411 in view of a published article by Garceau et al., "General Controls in a Local Area Network." Claims 1, 12-21, 23-27, and 32 have been rejected under 35 USC §102(b). All rejected claims are being appealed.

(iv) STATUS OF AMENDMENTS

No amendment has been filed after the final rejection mailed December 5, 2006.

(v) SUMMARY OF CLAIMED SUBJECT MATTER

Applicant's invention as claimed in independent claims 1 and 41 is directed to a method for securing software to reduce unauthorized use includes at least one hardware based authorized representative entity installed on or in a user device. As claimed in independent claim 78, Applicant's method associates at least one identifier with the software corresponding to a request for digital rights management and subsequently controls access to the software based on whether the user device is authorized without requiring a continuous connection with a remote authorized representative entity. The identifier feature of the invention is best illustrated in Figs. 62, 67, and 68 and described in Paras. [0291] and [0309] – [0314]. The identifier indicates that anti-piracy measures or copy protection is desired by the software distributor. The identifier may be in the form of a serial number, password, or other alphanumeric or binary string, for example and is preferably transparent to any systems that do not include an authorized representative or other module or device to implement copy protection so that the software may be used without restrictions on those systems or devices. As also described and illustrated in Figs. 67-68, the identifier may be included in a unique file prefix, file suffix, file extension, embedded within the content, or as a binary code, for example.

As illustrated and described with reference to Fig. 68, software that includes at least one identifier to trigger an authentication process on a user's system, network, or device is distributed to the user. The identifier is detected by an authorized representative entity that may be installed on or in the user device. The

authorized representative entity then determines whether attempted access to the software is authorized based on registration information and/or an authentication code associated with the software. The registration information and authentication code(s) may be associated with a particular user device or a group of authorized devices.

(vi) GROUNDS OF REJECTION TO BE REVIEWED

The rejection of Claims 1-99 under 35 USC §103(a) as being unpatentable over Ananda, U.S. Patent 5,495,411 in view of Garceau et al., "General Controls in a Local Area Network." is to be reviewed.

(vii) ARGUMENT

The Examiner rejected claims 1-99 as being unpatentable over Ananda (US5,495,411) in view of Garceau et al., "General Controls in a Local Area Newtork. However, neither Ananda nor Garceau et al. taken alone or in combination disclose or suggest an authorized representative entity installed on or in a user device as disclosed and claimed by Applicant. Similarly, neither reference relied upon by the Examiner taken alone or in combination discloses or suggests an identifier associated with the software corresponding to a request for digital rights management as disclosed and claimed by Applicant. For these reasons alone, Applicant's independent claims 1, 41, and 78 are patentable over combination of references proposed by the Examiner. As argued independently in greater detail below, a number of Applicant's dependent claims also include features that are neither disclosed nor suggested by the prior art relied upon by the Examiner such that Applicant respectfully requests that the rejection of claims 1-99 under 35 USC §103(a) be reversed.

As recited in independent claims 1, 41, and 78, Applicant's invention does not require a continuous connection with a remote authorized representative entity. In contrast, Ananda '411 discloses a secure software rental system that allows the user device to operate the software only while electronically connected to the central rental facility (Abstract) or while a continuous communication link is maintained between the first (rental facility) and second (user) computers by exchanging data at predetermined intervals, such as 30 seconds. (Col 2, ll, 48-50), for example. The Examiner relies on Garceau et al., which describes functions of a LAN administrator

who must be contacted by a user to establish a new password when the maximum interval has expired for the user's password being valid as disclosing this feature since the "user" is not required to be in continuous communication with the LAN administrator. Applicant respectfully disagrees with this interpretation of the teachings of Garceau et al. and the proposed combination with Ananda with respect to teaching a non-continuous connection with a remote authorized representative entity. Although the "communication" taught by Garceau et al. may be non-continuous, it is clearly "manual", "verbal" or "non-electronic" communication between two individuals whereas Applicant's disclosure as well as Ananda clearly apply to electronic communication between computers. As such, one of ordinary skill in the art would not interpret Garceau et al. as interpreted by the Examiner and would have no motivation to combine the features as proposed. The Examiner has not identified any proper motivation or suggestion to combine such features. Even if the combination were proper, the features of Garceau et al. when properly interpreted combined with those of Ananda do not teach or suggest all of the features of Applicant's independent claims 1, 41, and 78.

Applicant's independent claims 1 and 41 also include at least one hardware based authorized representative entity installed on or in a user device and determining whether the user device is authorized to access the software using the authorized representative entity installed on or in the user device. This feature is neither disclosed nor suggested by Ananda '411 nor by Garceau et al.

Applicant's independent claim 78 also includes associating at least one identifier with the software corresponding to a request for digital rights management. This feature is neither disclosed nor suggested by Ananda '411 nor by Garceau et al.

As per claim 2, Ananda does not disclose any feature that is self authenticating and self activating in conjunction with an authorized representative located on or in the user device as claimed. Ananda requires communication with a remote authorized representative to generate authorization verification passwords and is therefore not self activating and self authenticating as disclosed and claimed by Applicant.

As per claims 4-5, and 8 Ananda does not disclose a hardware based authorized representative entity installed on or in the user device and therefore does

not disclose using the representative entity to obtain registration information or to generate an authentication code as claimed by Applicant.

As per claims 9-10 Ananda does not disclose that registration information remains within a trusted network associated with the user device and is not disclosed to a third party. It is not clear from what the Examiner interprets as registration information disclosed by Ananda, but the information, passwords, authorization codes, etc. disclosed in Ananda are communicated between the user's computer and the third party central rental facility and do not remain within a trusted network of the user device as disclosed and claimed by Applicant.

Claims 11-13 are directed to alternative sequencing of obtaining registration information, generating authentication codes, etc. However, the Examiner relies on Ananda as disclosing all of these alternative sequences citing the same line numbers. Applicant respectfully submits that Ananda does not disclose the sequence of steps claimed in any of claims 11-13. Even conceding some interpretation of Ananda that could be construed to disclose one of the sequences, the remaining two are clearly not disclosed in Ananda.'411.

Claims 15-22 and 44-49 are directed to various features of a hardware based authorized representative entity. The Examiner relies on Col. 9, line 57 through col. 10, line 3 of Ananda, which describes the function of the Header Software. The header software disclosed by Ananda includes a rental security manager that must communicate with the central rental facility and exchange authorization information to allow the software application program to function. The header software is not a hardware based authorized representative entity as disclosed and claimed by Applicant. Likewise, the Examiner relies on Col. 6, lines 57-63 of Ananda describing the user computer 102 as including a processor and memory. However, this is not a hardware based authorized representative entity installed on or in the user device as disclosed and claimed by Applicant.

With respect to claims 25-26, and 29, the Examiner relies on Col. 3, lines 11-15 as disclosing that at least one authentication code is distributed with the software as claimed by Applicant. However, Ananda discloses that "the central rental facility requires the user to provide a unique user identification password to access the system. Each user of the system is allocated a unique user identification password." This clearly does not disclose distributing an authentication code with the software as claimed in claim 25 and is directly contrary to an authentication code

that corresponds to a group of user devices as claimed in claim 26. Claim 29 requires that the authentication code at least partially corresponds to a unique user device. In contrast, Ananda discloses that each user, not user device, is provided a unique password.

As per claims 27 and 28, the Examiner relies on Col. 9, lines 5-6, which states that "... the multiuser controller 222 registers a transfer time for the application software obtained from the timer clock of the database computer 122." This simply does not anticipate or suggest an authentication code that at least partially corresponds to a manufacturer of a user device or a model of a user device as claimed by Applicant.

As per claim 31, the Examiner relies on Col. 3, lines 16-49 which relates to the user entering a password to gain access to the central rental facility. If a valid password is not entered, communications with the user computer are terminated. This is taken out of context with respect to determining whether a user is authorized to access the software. As such, none of the steps of providing a hardware authorized representative entity, generating an authentication code, associating the authentication code, etc. are performed to control access to the software and this does not teach or suggest preventing transfer of the software to the current user device as claimed.

With respect to claims 33-34, the Examiner relies on Col. 10, lines 4-15 which describes one function of the header software in notifying the user of unauthorized use if the periodic test of whether the user is authorized fails. The header software operates on the user computer. There is no disclosure of a secondary user device as disclosed and claimed by Applicant. As such, there is no disclosure of performing the steps of obtaining, generating, and associating by a primary device and the steps of determining and controlling by a secondary device.

With respect to claim 37, Ananda does not disclose an identifier associated with the software to trigger authentication by an authorized representative entity. The header software disclosed by Ananda is executed without regard to whether authorization is requested.

With respect to claim 38, Ananda does not disclose securing any means for generating the authentication code after generating the authentication code associated with the software. While the authentication code may be encrypted, there is no disclosure of securing the software that generates the authentication code. To

the extent that the software is secured by being compiled or stored in binary executable form, it is not secured in that fashion after generating the authentication code as claimed by Applicant.

With respect to claim 39, the Examiner relies on Col 10, lines 8-15 of Ananda, which generally describe one function of the header software as terminating execution of the application software and notifying the user of unauthorized use if the periodic test fails. There is no disclosure of modifying the authorized representative entity to disable subsequent generation of authentication codes associated with the software while still performing the other steps of the method as claimed by Applicant.

With respect to claim 40, Ananda does not disclose generating an authentication code and associating the code prior to distribution of the software. Ananda uses the time of transfer of the software as recorded by the central rental facility and also the time as recorded by the user computer in generating the authentication codes and necessarily can not generate the authentication code prior to distribution of the software as claimed by Applicant.

With respect to claim 42, the header software disclosed by Ananda requires communication with the central rental facility and therefore is not self authenticating in conjunction with the authorized representative entity installed on or in the user device.

With respect to claims 51-57, the registration information disclosed by Ananda is associated with the user and not the user device. As such, Ananda does not disclose comparing registration information associated with the software to registration information associated with the user device as claimed by Applicant. Likewise, Ananda does not disclose registration information that includes hardware information, hardware information associated with a unique user device, a serial number, or hardware information associated with a group of user devices as claimed.

With respect to claims 58-61, the Examiner relies on Col.9, lines 35-36, which states "Once the transfer of an application software to the remote user computer system 150 is completed, the user is able to execute the application software on the user computer 102 of the remote user computer system 150 as though the user is independent of the central rental facility 180." It is unclear how this possibly anticipates or suggests a hardware based authorized representative entity installed

on or in the user device by a manufacturer of the user device as claimed by Applicant.

With respect to claim 62, Ananda does not disclose controlling access by preventing the software from being transferred to a second user device as claimed by Applicant. The only access control disclosed by Ananda is to terminate execution of the application program. Ananda clearly allows copying of the software to a second user device as described in Col.18, lines 55-64.

With respect to claim 64 Ananda does not disclose providing limited access to the software as claimed by Applicant. Rather, Ananda only discloses terminating the software if the use is unauthorized.

With respect to claim 66 Ananda does not disclose or suggest registration information associated with the user device. As previously described, the only registration information disclosed in Ananda is relative to the user, not the user device. As such, Ananda does not disclose or suggest generating at least one authentication code at least partially based on registration information associated with the user device as claimed by Applicant.

With respect to claim 68, Ananda does not disclose contacting a remote authorized representative entity if the authorized representative entity installed on or in a user device is unable to determine whether the user device is authorized as disclosed and claimed by Applicant. The central rental facility and header software disclosed by Ananda are both required at all times to perform any type of authorization or authentication functions. The header software continuously exchanges authentication codes with the central rental facility. There is no determination with respect to whether the software is authorized without contacting the central rental facility to obtain the current authentication code. Likewise, the header software can not determine whether the software is authorized without contacting the central facility. If the communication between the central rental facility and the header module is lost, the application program is terminated.

With respect to claim 69, Ananda does not disclose an authorized representative entity installed on or in the user device, and terminates the application software if it is unauthorized. As such, there is no disclosure or suggestion of contacting the remote authorized representative if the authorized representative entity installed on or in the user device determines that the user device is unauthorized.

With respect to claim 70, Ananda does not compare registration information associated with the user device with information encoded in an authentication code as claimed. The only registration information disclosed by Ananda is related to the user and user password used to gain access to the central rental facility.

With respect to claim 71, Ananda does not disclose a hardware based authorized representative entity installed on or in the user device and does not disclose any identifier that is detected by the authorized representative entity to trigger authentication functions. The authentication functions disclosed in Ananda are performed without regard to any type of identifier as disclosed and claimed by Applicant.

With respect to claims 72-77, Ananda does not disclose a triggering event to transfer information to the user computer and does not disclose updating an authorized representative entity installed on or in the user device as in Applicant's claim 74.

With respect to claim 79, the header module of Ananda is not self-activating and self-authenticating as claimed by Applicant because Ananda requires the header module to be in regular communication with the central rental facility.

With respect to claim 81, the registration information disclosed by Ananda is associated with a user, not a user device as claimed by Applicant. As such, Ananda does not disclose or suggest generating an authentication code based on the registration information as claimed by Applicant.

Claims 83-85 disclose alternative sequencing for generation of an authentication code relative to distribution of the software. However, the Examiner relies on a single disclosure in Ananda as disclosing all three alternatives, which is clearly not the case. The authentication code disclosed by Ananda is based on the transfer time of the software as determined by the central rental facility and the transfer time determined by the user computer. As such, Ananda does not generate the authentication code and associate the authentication code before distributing the software, concurrent with distributing the software, and after distributing the software as disclosed and claimed by Applicant.

With respect to claim 86, Ananda does not disclose an authorized representative entity installed on or in a user device and does not disclose registration information associated with at least one user device. As previously described, the registration information disclosed by Ananda is relative to the user

and is unique to the user, not the user device. As such , Ananda does not disclose an authorized representative entity installed on or in the user device that performs the functions claimed by Applicant.

With respect to claim 88, there is no disclosure or suggestion in Ananda of preventing the authorized representative entity installed on or in the user device from generating authentication codes for the software to secure the authentication code to resist user tampering as disclosed and claimed by Applicant. The only type of "securing" disclosed by Ananda is using encryption, or providing executable binary code. As previously described, this is different in kind from that claimed by Applicant.

With respect to claims 90 and 94, the central rental facility and header module of Ananda operate without regard to whether one or the other is present and operational. Similarly, the header module is downloaded every time the application program is downloaded and forms an integral part of the software downloaded to the user computer. There is no check to determine whether an authorized representative entity already exists locally or is installed on or in the user device. To the contrary, as described in Col. 17-19 of Ananda, the application software will not function if it was downloaded and stored in an earlier session and the user tries to connect to the central rental facility. As such, Ananda does not disclose or suggest determining whether an operational authorized representative entity is available locally as claimed.

With respect to claims 91-93, Ananda does not disclose or suggest an authorized representative entity installed on or in a user device and therefore does not disclose the methods for transferring an authorized representative entity to the user device as claimed by Applicant.

With respect to claim 95, Ananda discloses that the header module of the software communicates with the central rental facility to obtain the authentication codes. The header module then terminates the application software if the authentication codes calculated by the central rental facility do not match the authentication code determined by the user computer. As such, Ananda uses the header module and not the remote central rental facility to determine whether the user device is authorized and to control access to the software. Therefore, Ananda does not disclose that a remote authorized representative entity performs these functions as claimed by Applicant.

With respect to claims 96-98, the registration information disclosed by Ananda is related to the user, not the user device. There is no disclosure or suggestion of obtaining hardware specific registration information associated with a user device and generating at least one authentication code using the hardware specific information as claimed by Applicant.

With respect to claim 99, Ananda does not prevent the software from being transferred to the user device if the user device is not authorized. As previously described, the only action taken by Ananda is to terminate the software application program if the user is not authorized. Because the system/method disclosed by Ananda requires constant communication with the central rental facility, there is no motivation for Ananda to prevent such a transfer because the header module of the transferred software would terminate execution, even if a successful connection to the central rental facility is obtained as described in Col 17-19 of Ananda. As such, Ananda fails to disclose or suggest preventing the software from being transferred to the user device if the user device is not authorized.

SUMMARY

Applicant's invention as claimed in claims 1-99 includes a number of features that are neither disclosed nor suggested by Ananda or Garceau et al. taken alone or in any permissible combination. As such, Applicant's claims are patentable over the proposed combination and Applicant respectfully requests that the rejection under 35 USC §103(a) of claims 1-99 be reversed.

(viii) CLAIMS APPENDIX

1. (Previously Presented) A method for securing software to reduce unauthorized use, the method comprising:

providing at least one hardware based authorized representative entity installed on or in a user device;

obtaining registration information corresponding to at least one user device;

generating an authentication code at least partially based on the registration information;

associating the authentication code with the software;

determining whether a current user device is authorized based on the authentication code associated with the software and registration information associated with the current user device; and

controlling access to the software based on whether the current user device is authorized without requiring a continuous connection to a remote authorized representative entity.

2. (Original) The method of claim 1 wherein the software is self activating and self authenticating in conjunction with the hardware based authorized representative located on or in the user device.

3. (Original) The method of claim 1 wherein the software comprises data representing content selected from the group consisting of music, video, an application program, an operating system component, a game, a movie, graphics, watermarked works, a magazine, and a book.

4. (Original) The method of claim 1 wherein the step of obtaining registration information is at least partially performed by the at least one hardware based authorized representative entity installed on or in the user device.

5. (Original) The method of claim 1 wherein the step of generating an authentication code is at least partially performed by the at least one hardware based authorized representative entity installed on or in the user device.

6. (Original) The method of claim 1 wherein the step of obtaining registration information is performed by a remotely located authorized representative entity.

7. (Original) The method of claim 1 wherein the step of generating an authentication code is performed by a remotely located authorized representative entity.

8. (Original) The method of claim 1 wherein the steps of obtaining, generating, associating, determining, and controlling are at least partially performed by a resident hardware based authorized representative entity installed on at least one user device.

9. (Original) The method of claim 8 wherein registration information associated with the current user device remains within a trusted network associated with the user device.

10. (Original) The method of claim 8 wherein registration information associated with the current user device is not communicated to any third party.

11. (Original) The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed prior to transferring the software to the current user device.

12. (Original) The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed substantially concurrently with transferring the software to the current user device.

13. (Original) The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed following transferring the software to the current user device.

14. (Original) The method of claim 11 wherein the steps of obtaining, generating, and associating are performed by a remote authorized representative entity.

15. (Original) The method of claim 1 wherein the hardware based authorized representative functions are hard coded.

16. (Original) The method of claim 1 wherein the hardware based authorized representative functions are programmable.

17. (Original) The method of claim 1 wherein the hardware based authorized representative functions are both hard coded and programmable.

18. (Original) The method of claim 1 wherein the hardware device is a computer chip.

19. (Original) The method of claim 1 wherein the hardware device is integral with a CPU.

20. (Original) The method of claim 1 wherein the hardware device is a PC card.

21. (Original) The method of claim 1 wherein the hardware device is a microprocessor.

22. (Original) The method of claim 1 wherein the steps of determining whether a current user device is authorized and controlling access to the software are at least partially performed by the hardware based authorized representative entity installed on or in a user device.

23. (Original) The method of claim 1 wherein the software is electronically distributed.

24. (Original) The method of claim 1 wherein the software is transferred to a user device from a computer readable storage medium.

25. (Original) The method of claim 1 wherein at least one authentication code is distributed with the software.

26. (Original) The method of claim 1 wherein the authentication code corresponds to a group of user devices.

27. (Original) The method of claim 26 wherein the authentication code at least partially corresponds to a manufacturer of a user device.

28. (Original) The method of claim 26 wherein the authentication code at least partially corresponds to a model of a user device.

29. (Original) The method of claim 1 wherein the authentication code at least partially corresponds to a unique user device.

30. (Original) The method of claim 1 wherein the steps of determining whether a current user device is authorized and controlling access to the software are performed by a remotely located authorized representative entity.

31. (Original) The method of claim 1 wherein the step of controlling access to the software comprises preventing transfer of at least a portion of the software to the current user device.

32. (Original) The method of claim 1 wherein the step of controlling access to the software comprises preventing the current user device from utilizing the software.

33. (Original) The method of claim 1 wherein the steps of determining and controlling are at least partially performed by an authorized representative installed on a secondary user device.

34. (Original) The method of claim 1 wherein the steps of obtaining, generating, and associating are performed by a primary user device and the steps of determining and controlling are performed by a secondary user device.

35. (Original) The method of claim 1 further comprising encrypting the authentication code.

36. (Original) The method of claim 1 further comprising encrypting the registration information.

37. (Original) The method of claim 1 further comprising associating an identifier with the software to trigger authentication by an authorized representative entity.

38. (Original) The method of claim 1 further comprising:
securing any means for generating the authentication code after generating the authentication code associated with the software.

39. (Previously Presented) The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are at least partially performed by a hardware based authorized representative entity installed on or in a user device, the method further comprising:

modifying the authorized representative entity to disable subsequent generation of authentication codes associated with the software.

40. (Original) The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed by a remote authorized representative prior to distribution of the software.

41. (Previously Presented) A method for securing software to reduce unauthorized use having a hardware based authorized representative entity installed on or in a user device, the method comprising:

determining whether the user device is authorized to access the software using the authorized representative entity; and

controlling access to the software based on whether the user device is determined to be authorized without a continuous connection to a remote authorized representative entity.

42. (Original) The method of claim 41 wherein the software is self authenticating in conjunction with the authorized representative located on or in the user device.

43. (Original) The method of claim 41 further comprising:

determining whether the user device is authorized to access the software using a remotely located authorized representative entity in combination with the authorized representative entity installed on or in the user device.

44. (Original) The method of claim 41 wherein the hardware based authorized representative functions are hard coded.

45. (Original) The method of claim 41 wherein the hardware based authorized representative functions are programmable.

46. (Original) The method of claim 41 wherein the hardware based authorized representative functions are both hard coded and programmable.

47. (Original) The method of claim 41 wherein the hardware based authorized representative entity comprises a computer chip.

48. (Original) The method of claim 41 wherein the hardware based authorized representative entity is integral with the CPU.

49. (Original) The method of claim 41 wherein the hardware based authorized representative entity comprises a PC card.

50. (Original) The method of claim 41 wherein the hardware based authorized representative entity comprises program instructions executed by a microprocessor.

51. (Original) The method of claim 41 wherein the step of determining whether the user device is authorized comprises:

comparing registration information associated with the user device to registration information associated with the software.

52. (Original) The method of claim 51 wherein the registration information associated with the software is embedded within an authentication code.

53. (Original) The method of claim 51 wherein the registration information associated with the software is encrypted.

54. (Original) The method of claim 51 wherein the registration information includes hardware information.

55. (Original) The method of claim 54 wherein the registration information includes hardware information associated with a unique user device.

56. (Original) The method of claim 55 wherein the hardware information includes a serial number.

57. (Original) The method of claim 54 wherein the registration information includes hardware information associated with a group of user devices.

58. (Original) The method of claim 41 wherein the hardware based authorized representative entity is installed by a manufacturer of the user device.

59. (Original) The method of claim 41 wherein the hardware based authorized representative entity is installed from a computer readable storage medium.

60. (Original) The method of claim 41 wherein the hardware based authorized representative entity is downloaded to the user device.

61. (Original) The method of claim 60 wherein the authorized representative entity is transferred to the user device from a network.

62. (Original) The method of claim 41 wherein the step of controlling access comprises preventing the software from being transferred to a second user device.

63. (Original) The method of claim 41 wherein the step of controlling access comprises preventing the software from being executed by the user device.

64. (Original) The method of claim 41 wherein the step of controlling access comprises providing limited access to the software.

65. (Original) The method of claim 41 wherein the software comprises data representing content selected from the group consisting of music, video, an application program, an operating system component, a game, a movie, graphics, watermarked works, a magazine, and a book.

66. (Original) The method of claim 41 wherein the software comprises instructions for generating at least one authentication code at least partially based on registration information associated with the user device.

67. (Original) The method of claim 66 wherein the software comprises instructions for encrypting the authentication code.

68. (Original) The method of claim 41 wherein the step of determining whether the user device is authorized comprises:

contacting a remote authorized representative entity if the authorized representative entity installed on or in a user device is unable to determine whether the user device is authorized.

69. (Original) The method of claim 41 wherein the step of determining whether the user device is authorized comprises:

contacting a remote authorized representative if the authorized representative entity installed on or in a user device determines that the user device is not authorized.

70. (Original) The method of claim 41 wherein the step of determining whether the user device is authorized comprises:

obtaining registration information associated with the user device; and

comparing the registration information associated with the user device with registration information encoded in an authentication code associated with the software.

71. (Original) The method of claim 41 further comprising:

detecting an identifier associated with the software to trigger authentication functions performed by the hardware based authorized representative entity installed on or in the user device; and

performing the steps of determining whether the user device is authorized and controlling access to the software only if the identifier is detected.

72. (Original) The method of claim 41 further comprising:

automatically contacting a remote authorized representative based upon a triggering event to receive information.

73. (Original) The method of claim 72 wherein the information is selected from a group consisting of updates, upgrades, patches, marketing information, promotional information, quality assurance information, network monitoring and metering information, and error and usage information.

74. (Original) The method of claim 73 wherein the information updates the authorized representative entity installed on or in the user device.

75. (Original) The method of claim 73 wherein the information modifies the software.

76. (Original) The method of claim 72 wherein the triggering event is based on a user action.

77. (Previously Presented) The method of claim 72 wherein the automatic contact with the remote authorized representative is repeated.

78. (Original) A method for reducing unauthorized use of software, the method comprising:

associating at least one identifier with the software corresponding to a request for digital rights management;

distributing the software to a user;

detecting the at least one identifier using an authorized representative entity;

associating at least one authentication code with the software;

determining whether a user device is authorized to access the software; and

controlling access to the software based on whether the user device is authorized without requiring a continuous connection with a remote authorized representative entity.

79. (Original) The method of claim 78 wherein the software is self activating and self authenticating in conjunction with a hardware based authorized representative located on or in the user device.

80. (Original) The method of claim 78 further comprising encrypting the at least one authentication code.

81. (Original) The method of claim 78 further comprising:

obtaining registration information associated with at least one user device; and

generating the at least one authentication code at least partially based on the registration information.

82. (Original) The method of claim 67 further comprising encrypting the registration information.

83. (Original) The method of claim 81 wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed before the step of distributing the software.

84. (Original) The method of claim 81 wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed substantially concurrently with the step of distributing the software.

85. (Original) The method of claim 81 wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed subsequent to the step of distributing the software.

86. (Original) The method of claim 81 wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed by an authorized representative entity installed on or in the user device.

87. (Original) The method of claim 81 wherein the step of generating the at least one authentication code is performed by an authorized representative entity installed on or in the user device, the method further comprising:

securing the authentication code to resist user tampering.

88. (Original) The method of claim 87 wherein the step of securing comprises preventing the authorized representative entity installed on or in the user device from generating any more authentication codes for the software.

89. (Original) The method of claim 87 wherein the step of securing comprises encrypting the authentication code.

90. (Original) The method of claim 78 further comprising:

determining whether an operational authorized representative entity is available locally;

installing an authorized representative entity on or in the user device if an operational authorized representative entity is not available locally.

91. (Original) The method of claim 90 wherein the step of installing comprises transferring the authorized representative entity to the user device from a remote authorized representative entity.

92. (Original) The method of claim 90 wherein the step of installing comprises transferring the authorized representative entity to the user device from a computer readable storage medium.

93. (Original) The method of claim 90 wherein the software includes an authorized representative entity and wherein the step of installing comprises transferring the authorized representative entity to the user device from the software.

94. (Original) The method of claim 78 further comprising:

determining whether an operational authorized representative entity is installed on or in the user device; and

contacting a remote authorized representative entity if no operational authorized representative entity is installed on or in the user device.

95. (Original) The method of claim 94 wherein the remote authorized representative entity performs the steps of determining whether a user device is authorized and controlling access to the software.

96. (Original) The method of claim 78 further comprising:

obtaining registration information including hardware specific information associated with a user device, wherein the steps of obtaining registration information and associating at least one authentication code are performed prior to the step of distributing the software to a user.

97. (Original) The method of claim 78 further comprising:

obtaining registration information including hardware specific information associated with a user device, wherein the steps of obtaining registration information and associating at least one authentication code are performed substantially concurrently with the step of distributing the software to a user.

98. (Original) The method of claim 78 further comprising:

obtaining registration information including hardware specific information associated with a user device, wherein the steps of obtaining registration information and associating at least one authentication code are performed following the step of distributing the software to a user.

99. (Original) The method of claim 67 wherein the step of controlling access to the software comprises preventing the software from being transferred to the user device if the user device is not authorized.

(ix) EVIDENCE APPENDIX

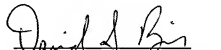
Not Applicable

(x) RELATED PROCEEDINGS APPENDIX

Not Applicable

Please charge any additional fees or apply any credits to **Deposit Account 50-2841 (Bir Law, PLC)**.

Respectfully submitted:



David S. Bir (Reg. No. 38,383)

Dated; December 5, 2007

Bir Law, PLC
13092 Glasgow Ct.
Plymouth, MI 48170